Best Available Copy

REMARKS

Applicants respectfully request reconsideration and allowance of the present application based on the foregoing amendments and following remarks. By this amendment, claims 1, 2, 21, 27 have been amended, and new claims 31-33 have been added. Claims 1, 2, 9, 21, 22 and 27-33 are pending in the application.

Claim Objections

Claims 1 and 21 were objected to because certain new limitations were not considered to be clearly defined/supported in the original disclosure. These limitations are addressed separately below.

"the web page object to be automatically rendered and displayed"

It is submitted to be notoriously well known that a browser automatically renders objects that are included in web pages accessed by the browser (e.g. by entering a URL in a browser). It is also submitted to be well known that web pages hosted by a web site can include objects that are hosted at other locations on the Internet (e.g. objects such as .GIF files located at a different URL than the web site). So when the browser accesses a page associated with the website requested by the visitor, and encounters the reference to the foreign object, the browser automatically requests the web page object using the different URL, then automatically renders and displays its contents.

The specification is replete with references to the use of web pages, web sites and browsers, and their well-known aspects. For example, at page 2, lines 11-13, the specification states that "Visitor 106 is a consumer or other interested party visiting, or contemplating visiting, website(s) 104 or other Internet service provided by service 102 via a PC and a modem, web kiosk or other Internet access device."

Also, at page 8, lines 5-8, the specification teaches:

> Generally, on-line service 102 has entered into an agreement with the security system to perform third-party security verification services for one or more website(s) 104 they operate, the results of which are further available for viewing by its visitors 106 in a simple manner as described in more detail below.

PAGE 9/31 * RCVD AT 12/11/2007 8:47:31 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:6502334545 * DURATION (mm-ss):05-32

Best Available Copy

Still further, at page 13, lines 1-6:

> Verification engine 310 [of system 200] provides security status information of registered services 102 to visitors 106. For example, once the scanning engine 302 has completed the scanning process and results of the process have been uploaded, the customer information database 304 is updated with a security status. In one example implementation, a service 102 that has been registered with system 200 places a "Bug" (e.g. a GIF or other image file with an associated URL or script, i.e. hyperlink) in web pages presented by its website(s) 104.

Also, at page 13, line 21 to page 14, line 4:

> It should be noted that security status information can be provided to visitors of website 104 in a variety of ways in addition to a bug provided on a page of website 104 that clicks through to a simple rating page. For example, verification engine 310 can cause the bug to click through to a detailed security meter page such as will be described in more detail below. As another example, the verification engine 310 can cause an up-to-date security status to be provided directly on the page in place of the bug, for example by continuously updating a .GIF file accessed by the website.

This last described embodiment, wherein a continuously updated image file (e.g. .GIF file) is hosted by system 200 and accessed by direct reference in pages of website 104, is the focus of amended independent claim 1.

"in a first verification operation prior to the visitor's access request"

"in a second verification operation prior to the visitor's access request"

It is submitted that this claimed subject matter is readily apparent to one skilled in the art reading the specification. Moreover, as set forth above, the specification teaches that at page 13, line 21 to page 14, line 4 (emphasis added):

> It should be noted that security status information can be provided to visitors of website 104 in a variety of ways. . . . As another example, the verification engine 310 can cause an up-to-date security status to be

PAGE 10/31 * RCVD AT 12/11/2007 8:47:31 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:6502334545 * DURATION (mm-ss):05-32

Best Available Copy

> provided directly on the page in place of the bug, for example by continuously updating a .GIF file accessed by the website.

Accordingly, it should be apparent that verification engine 310 can periodically and/or repeatedly perform verification operations of a service so that subsequent access requests to its websites 104 have "up to date" security status levels (i.e. different accesses can yield different security status, depending on the immediately preceding verification operation, which can occur "continuously").

Moreover, at page 13, lines 11-18, the specification teaches:

> In a further example implementation, rather than just presenting the saved security status from database 304 to the visitor 106, the security status presented to visitor 106 can be extrapolated to the moment of the visitor's request. Such an up-to-date security status can be derived by checking the number of vulnerabilities over a certain severity level stored in database 304 for the requested service 102 and applying a grace period for the service 102 to resolve the problem. If sufficient vulnerabilities exist for a long enough period of time, for example, a non-encrypted FTP service is running on the website 104 for more than 48 hours, the security status of service 102 can be downgraded.

This provides another example that demonstrates how a security status can be computed and stored before (i.e. prior to) requests to access a website 104 are made by visitors, and independently from those access requests.

"different security status levels via the automatic rendering of the prior-determined web page object contents"

As shown above, it should be apparent to those skilled in the art from reading the specification how a web page object automatically rendered by a visitor's browser can provide the security status of the website. Moreover, as shown above, the specification teaches that "the verification engine 310 can cause an up-to-date security status to be provided directly on the page in place of the bug, for example by continuously updating a .GIF file accessed by the website." It should be apparent, therefore, that the specification describes changing the contents of a web page object, thereby providing potentially different security status levels to a visitor

PAGE 11/31 * RCVD AT 12/11/2007 8:47:31 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:6502334545 * DURATION (mm-ss):05-32

Best Available Copy

through the automatic rendering of the object by a browser, depending on when the visitor accesses the website.

"wherein the first and second verification operations to determine the on-line service's security status and control . . . are performed by the verification service prior to and completely independent from the visitor's request to access . . . and independently from any action by the visitor and the visitor's browser"

As shown above, the specification teaches that "the verification engine 310 can cause an up-to-date security status to be provided directly on the page in place of the bug, for example by continuously updating a .GIF file accessed by the website." This clearly means that verification operations (e.g. "continuous") of a service having a website are independent from visitor access requests. One skilled in the art reading the specification would clearly understand that the "continuous" verification operations do not depend on a visitor's access request or actions.

In one example, the verification operations to calculate a security status level can be performed periodically, as configured by a on-line service. For example, the specification teaches at page 18 lines 1-11 that:

> An example of how new threats can be entered into the system will now be explained in even further detail. For example, system 200 can include a process that periodically sends a request for new and updated vulnerability test scripts from nessus.org. . . . The vulnerability fingerprint record can then be used by the alert engine to compare against fingerprint information for all customer devices stored in the customer information database to see if the customer may possibly be exposed to the newly threat. The vulnerability fingerprint record also contains information to identify the severity of the vulnerability, which can be used to calculate the security status for the customer, as will be explained in more detail below.

The specification clearly teaches that these verification operations are operations of the system 200, which operates independently of any visitor access requests and is not necessarily dependent on any actions by visitors or their browsers.

"appears invisible to the visitor after it is rendered by the visitor's browser"

PAGE 12/31 * RCVD AT 12/11/2007 8:47:31 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:6502334545 * DURATION (mm-ss):05-32

Best Available Copy

As shown above, the specification teaches that "the verification engine 310 can cause an up-to-date security status to be provided directly on the page in place of the bug, for example by continuously updating a .GIF file accessed by the website."

In one example, the .GIF file can be controlled to be a single-dot clear GIF file, which will appear invisible when rendered by a browser. See the present specification at, for example, page 24, lines 7-11.

For at least the reasons provided above, it is respectfully submitted that the objections to the claims should be withdrawn.

Double Patenting

Claims 1, 2, 9, 21, 27, 28, 29 and 30 are provisionally rejected for obvious-type double patenting in view of claims 1, 2, 9, 39 and 40 of U.S. Patent Appln. No. 10/113,875 in view of U.S. Patent No. 6,658,394 to Khaishgi et al. ("Khaishgi"). Although Applicants respectfully disagree with the basis for this rejection, Applicants reserve the right to file a terminal disclaimer to overcome this rejection.

Claim Rejections Under 35 U.S.C. 102

Claims 1, 21, 29 and 30 stand rejected under 35 U.S.C. 102(e) as being anticipated by Khaishgi. For reasons more fully set forth below, this rejection is respectfully traversed.

Independent claims 1 and 21 have been further amended to even more clearly define certain aspects of a verification service according to the invention, and require, inter alia:

> a web page object that is automatically rendered by a browser when a visitor uses the browser to access one or more web pages of the on-line service via a public network; and
> a verification service that hosts and controls contents of the web page object,
> . . .
> wherein the levels of the security status displayed for the visitor via the automatic rendering of the web page object indicate how vulnerable devices and services of the on-line service are to hackers and other online security threats as determined by the first and second verification operations, and
> wherein at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new

PAGE 13/31 * RCVD AT 12/11/2007 8:47:31 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:6502334545 * DURATION (mm-ss):05-32

Best Available Copy

vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services.

Khaishgi does not teach and would not have suggested the invention of amended independent claims 1 and 21.

Khaishgi teaches a seal issuing and certification service that allows merchants to place "seals" on their web pages. These seals are intended to be associated "with certain qualities such as trustworthiness, reliability and superior customer service." (col. 2, lines 56-66).

Khaishgi provides a "seal issuer 8" that merely "verifies the credentials, policies or business practices" of merchants desiring a seal. (col. 2, lines 44-45). However, nowhere does Khaishgi teach or suggest the verification operations as explicitly defined by amended independent claims 1 and 21, which provide an indication of "how vulnerable devices and services of the on-line service are to hackers and other online security threats." Still further, Khaishgi does not teach or suggest that "at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services."

Accordingly, Khaishgi does not disclose or suggest at least the following limitations of amended independent claims 1 and 21:

[1] wherein the levels of the security status displayed for a visitor via the automatic rendering of the web page object indicate how vulnerable devices and services of the on-line service are to hackers and other online security threats as determined by the first and second verification operations, and

[2] wherein at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services.

PAGE 14/31 * RCVD AT 12/11/2007 8:47:31 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:6502334545 * DURATION (mm-ss):05-32

Best Available Copy

For at least the above reasons, amended independent claims 1 and 21 patentably define over the cited prior art. Accordingly, the rejection of claims 1 and 21, together with claims 29 and 30 that depend from claim 21, should be withdrawn.

Claim Rejections Under 35 U.S.C. 103 in view of Khaishgi and Pham

Claims 2, 9, 27 and 28 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Khaishgi in view of U.S. Patent Pub. No. 2003/0097591 of Pham et al. ("Pham").

Claims 2, 9 ultimately depend from claim 1, and claims 27 and 28 depend from claim 21 and so they are all patentable over Khaishgi for at least the reasons presented above. The alleged combination of Khaishgi with Pham would not cure the deficiencies noted above. Indeed, the Office Action only alleges that Pham teaches evaluating vulnerability scans of the service to determine a security status level. Pham does not suggest that "at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services." Accordingly, claims 2, 9, 27 and 28 are patentable for at least the reasons claims 1 and 21 are patentable.

For at least these reasons, the § 103 rejection of claims 2, 9, 27 and 28 should be withdrawn.

Newly Added Claims

Claims 31-33 have been added to more fully define patentable features as originally disclosed in the specification, including the passages noted above in connection with the objections to the claims. They further patentably define over the cited prior art.

PAGE 15/31 * RCVD AT 12/11/2007 8:47:31 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:6502334545 * DURATION (mm-ss):05-32

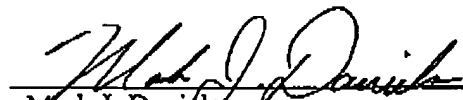
Best Available Copy

Conclusion

All objections and rejections having been addressed, it is respectfully submitted that the present application is in a condition of allowance and a Notice to that effect is earnestly solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: December 11, 2007



40,580
Reg. No.

Mark J. Danielson
(650) 233-4777
Please reply to customer no. 27,498

PAGE 16/31 * RCVD AT 12/11/2007 8:47:31 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:6502334545 * DURATION (mm-ss):05-32